Abstract: We attempt to show that, there are infinitely many Fermat Primes, by using Schröder - Bernstein’s Theorem, another known results in Arithmetic and Number Theory.

Keywords. Fermat Primes(Quadratics Forms), Fermat Primes(classic forms), Pomerance’s Theorem, Cantorian Set Theory.

SMC 2010: 11AXX

1. Introduction.

Leonhard Euler (1707-1783) showed that P. Fermat (1601-1665), was wrong about primality of the number $F_5$; this fact is so well known, that we not need insist on it[7].In any way, accordingly Historians of Mathematics. P de Fermat it’ is justly considered a pioneer theorist in Number Theory[12].It’s well known today that, English Mathematician,Dr. Andrew Wiles, proved(1994), the famous marginal note so-called “Fermat Last’s Theorem, namely justly Fermat-Wiles Theorem[13].

2. Notation and Assumptions.

2.1 Starting with, we need distinguishing Fermat Primes (classic form) their Fermat Primes (quadratic form). More formally, as is usual in Number Theory we will denote Fermat Primes by employing the set below:

1. $F_p = \left\{ f \in \mathbb{N} : f = 2^{2^n} + 1, \text{ where } n \in \mathbb{N} \text{ and } f \text{ is prime} \right\}$, [18].

Whereas the symbol $Q'_p$ denotes Fermatian Primes or quadratic forms, this subset of $\mathbb{N}$ plays an very important role in our proof. In such case, we can write more explicitly,

2. $Q'_p = \left\{ x \in \mathbb{N} : x = n^2 + 1, n \in \mathbb{N} \right\}$, but $x$ is to be a prime number.

2.2 For the sake of completeness, also we need assume (without proof) some known results in Arithmetic, Algebra and Set Theory:

Lemma 1. Schröder – Bernstein’s Theorem.
Let \( F : \Phi \to \Omega \) and \( G : \Omega \to \Phi \) be injective functions, then there exists a Bijective function \( \Theta : \Omega \to \Phi \), [4].

Lemma 2. Cantor’s Theorem.
If \( \Psi : S \to T \) is a biyective function, thus \( \text{Card} . ( S ) = \text{Card} . ( T ) \), [2].

Lemma 3. Pomerance’s Theorem. Every prime \( p \), has a proof of its primality, [5].


3.1.- Before coming to the proof, we need build a natural generating function in the following way; Let \( \varphi : \mathbb{N} \to \mathbb{N} \) be defined by the formula below:

\[
\varphi(n) = \begin{cases} 
2^n + 1 & \text{if and only if } 2^n + 1 \text{ is prime} \\
\text{n}^2 + 1 & \text{otherwise}
\end{cases}
\]

Proposition 3.1. The set of images of the function \( \varphi(n) \), namely \( I_\varphi \), does contain in particular two infinite subsets: Fermat Primes \( F_n \) and \( \mathbb{N} - F_n = Q'_p \), where \( Q'_p \) represents the natural sequence of primes defined at (2) above.

Proof.
Firstly, we must prove the fact that \( Q'_p \) is not finite.

Notice that, recently (in the twenty one century) has been proved that \( \text{Card} . ( Q'_p ) = \aleph_0 \), [3].

Further, in particular \( Q'_p \) contains all Fermat Primes (quadratic forms) and we may write: \( Q'_p \subset I_\varphi \), whenever \( I_\varphi \) stands for the set of images of the function \( \varphi(n) \) defined at (1), from this we can see,

\[
\text{Card} . ( Q'_p ) = \aleph_0 , \text{ as asserted.}
\]

3.2 Next, we are going to prove our main result: \( \text{Card} . ( F_n ) \) is not finite[11]. In order to solve our guess, let \( I_n \) be a auxiliary set: \( I_n = \{ x \in \mathbb{N} : x = 2^n , n \in \mathbb{N} \} \).

Obviously, \( \text{Card} . ( I_n ) = \aleph_0 \), and by construction, one has the relation:

\[
\text{Card} . ( I_n ) = \text{Card} . ( Q'_p ) = \text{Card} . ( \mathbb{N} ) = \aleph_0 .
\]

In the rest of this short article, \( L_n x \) means: Logarithm natural of \( x \), [20].

We shall use the following properties of \( I_n \): every \( x \in I_n \) can be written by using the set \( Q'_p \). Of course, we can proceed in the following way:

Let \( x \) an arbitrary member of \( Q'_p \), thus we have that Diophantine equation:
(4) \( x = n^2 + 1 \) for some \( n \in \mathbb{N} \), hence we can write \( x - 1 = n^2 \), so one has,

(5) \( n^2 = x - 1 \Rightarrow \left[ (L_n n)^{-1} \cdot L_n \ (x - 1) \right] = 2^n \in I_n \).

In fact, we have infinite possibilities for the choice of \( n \) belonging to \( Q^f_p \).

Furthermore, from (4) we can see, \( x = n^2 + 1 \Rightarrow n = \left( x - 1 \right)^{1/2} \) consequently,

(6) \( 2^n = 2^{\sqrt{x-1}} \Rightarrow 2^{2n} = 2^{2\sqrt{x-1}} \), that is to say; \( 2^{\sqrt{x-1}} = 2^n \), therefore we have,

(7) \( 2^{\sqrt{x-1}} + 1 = 2^n + 1 = f \in F_n \), which tell us that \( f \in F_n \) or not, according to for

when \( x \in Q^f_p \). This assertion has unique answer computationaly (in accordance with Lemma 3 above or Pomerance’s Theorem).

Unfortunately, not all Fermatian Primes (quadratic forms) generates Fermat’s Primes, which we need prove the following statement:

**Proposition 3.2** Let \( \psi_1 : I_n \to F_n \) and \( \psi_2 : F_n \to I_n \), be defined by the system,

(8) \[
\begin{align*}
\psi_1(x) &= 2^x + 1 = 2^{2n} + 1 \\
\psi_2(f) &= \log_2(f - 1)
\end{align*}
\]

Then \( \psi_1 \) and \( \psi_2 \), so constructed are both injective functions.

**Proof.**

2.i.- Let us assume that \( x_1, x_2 \) both belong to \( I_n \), whence there are natural numbers \( n_1, n_2 \) such that :

(9) \( x_1 = 2^{n_1} \), and at the same time, \( x_2 = 2^{n_2} \), suppose \( \psi_1(x_1) = \psi_1(x_2) \), next \( 2^{n_1} + 1 = 2^{n_2} + 1 \Rightarrow 2^{n_1} = 2^{n_2} \), from this we may write: \( 2^{n_1} = 2^{n_2} \) or \( x_1 = x_2 \).

Thence, we have obtained that \( \psi_1 \) is an injective function, as asserted.

2.i.i. Analogously, let us \( f_1 \) and \( f_2 \) belonging to \( F_n \). We can assume that \( f_1 \neq f_2 \) and \( f_1 < f_2 \) (or \( f_2 < f_1 \), the treatment is the same, without changing it in any essential way).

According to our hypothesis we can write the following immediate inequalities:

(10) \( f_1 - 1 < f_2 - 1 \), because \( f_1 \) and \( f_2 \) are both positive numbers, thus we obtain the relation, \( \log_2(f_1 - 1) < \log_2(f_2 - 1) \), but by applying (8), this last inequality takes the form below:
4. Important Results.

4.1. Finally we can pay attention to our aim in this brief research work.

**Proposition 4.1:** $\text{Card.}(F_n) = \mathbb{N}_0$. To prove this statement is sufficient to study carefully the cardinality of the sets $F_n$ and $Q_p^f$ simultaneously. In fact, can occur only four possibilities:

**Case 1:** If $F_n$ and $Q_p^f$ are both finite sets; in particular $Q_p^f$ should be finite, but we have proved at Proposition 3.1 that $\text{Card.}(Q_p^f) = \mathbb{N}_0$, therefore we have obtained a contradiction, so this case is not possible.

**Case 2:** If $Q_p^f$ is infinite and $F_n$ finite. Since $F_n$ is finite, it follows that there exists a biggest Fermat Prime says,

$$f_n^* = 2^{2^n} + 1$$

for some huge number $n^* \in \mathbb{N}$. This means that:

$$\forall n > n^*, \text{ numbers of the form } f_n = 2^{2^n} + 1 \text{ are all composite, therefore, we may write that increasing and finite sequence:}$$

$$f_1, f_2, f_3, \ldots, f_{i-1}, f_i, f_{i+1}, \ldots, f_\lambda.$$ It is obvious that, by hypotheses the relation

$$\text{Card.}(F_n) = \lambda \in \mathbb{N}, \text{ holds.}$$

4.2. Recall that $\psi_1 : I_n \rightarrow F_n$ and $\psi_2 : F_n \rightarrow I_n$ are both injective functions (Proposition 3.2); then there exists a **Bijective** function $\theta : I_n \rightarrow F_n$, by using Lemma 1 or Schröder-Bernstein’s Theorem, this is same thing as say that,

$$\text{Card.}(F_n) = \text{Card.}(I_n), \text{ in accordance with Lemma 2 or Cantor’s Theorem.}$$

Clearly (14) contradicts (13), because we have stated at (3) that $\text{Card.}(I_n) = \mathbb{N}_0$, also this case must be naturally discarded.

**Case 3:** Assume $F_n$ infinite and $Q_p^f$ is finite. Similarly to Case 1, we have again a contradiction with Proposition 3.1 above.

4.3. At this point of the proof, all that remains is to discuss the last possibility:

**Case 4:** When $F_n$ and $Q_p^f$ are both infinite sets. This Hypotheses does not contradicts, any of the previous Theorems or assumptions made in this notes.
However, taking into account that, all possible cases have been examined, we conclude that, sequence of primes of the form \( f_n = 2^{2^n} + 1 \) never ends; this is another way of saying that, Fermat’s Prime numbers go on forever, therefore:

\[
(15) \quad \text{Card}(F_n) = \aleph_0,
\]

as was to be proved.

5. Concluding comments

In the current literature \[6\], the higher Fermat numbers have been the subject of prolonged study, to date no more primes have been found among them \[8\][23]. In other words, \( F_n \) generates primes and composite numbers at random. Although, we believe that, the next Fermat prime (for \( n \) greater than 5) would be a so huge number \[21][22\] and probably our modern computers \[9\], don’t have sufficient memory capacity to contain it \[15][17\].

6. Acknowledgements

El Autor de este modesto aporte, expresa las más sinceras gracias, a la Dra. Alicia Fernanda Parra de Ortiz, Presidenta del Consejo Superior de la Universidad; por todo su apoyo Logístico, para la culminación del presente logro académico.

Así mismo quiero destacar, el constante respaldo moral, por parte de la Prof. y Colega: PhD. Clara González Silva, quien tiene a su cargo, la Dirección de Investigación y Proyectos de la Universidad José María Vargas /Caracas-Venezuela.

7. References


